IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF:	*	Complaint: 1:21-mj-442 TMD
THE TARGET DEVICE SEIZED FROM 6202 CEDAR DRIVE APARTMENT D, CURRENTLY AT THE HSI BALTIMORE COMPUTER LAB 40 SOUTH GAY STREET, ROOM 427 BALTIMORE, MARYLAND, 21202	*	[redacted]
THE APPLE ACCOUNTS: COLDHEARTED1219@GMAIL.COM WITH DS ID 11764867435 TWOTHREE04@ICLOUD.COM WITH DS ID 17283723117	*	
THE GOOGLE ACCOUNT: COLDHEARTED1219@GMAIL.COM	*	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Peter T. Baish, a Special Agent (SA) with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

1. I have been an Agent since June 2003. As part of the daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, U.S.C. §§ 2251 and 2252A. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received formal training through HSI and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material, and internet crime. I have participated in the execution of numerous search warrants, of which the majority has involved child

exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including various sections of Title 18, United States Code § 2252A involving child exploitation offenses. I have also participated in the execution of search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with HSI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

2. I have received formal training from HSI and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material and Internet crime. This includes, but is not limited to, use of internet facilities to produce child pornography in violation of 18 U.S.C. § 2251(a), distribute and receive child pornography in violation of 18 U.S.C. § 2252(a)(2) and possess child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B).

3. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to affect arrests and execute warrants issued under the authority of the United States.

4. This affidavit is being is being submitted in support of applications for warrants to search the following:

a. The following "TARGET DEVICE" (See Attachments A1 and B1): **Apple iPhone 7, IMEI: 354916095756655**;

b. The following "TARGET ACCOUNTS":

i. The Apple, Inc. account associated with the email address **coldhearted1219@gmail.com** and DS ID 11764867435, and the Apple, Inc. account associated with the email address **twothreetwo04@gmail.com** and DS ID 17283723117 (See Attachments A2

and B2);

ii. The Google Inc. account associated with the email address **coldhearted1219@gmail.com** (See Attachments A3 and B3).

Collectively referred to as the TARGET LOCATIONS. The TARGET LOCATIONS are to be searched for evidence of violations of Title 18, United States Code, Section 2251(a) (production of child pornography), Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography), and 18 U.S.C. § 922(g) (Possession of a Firearm by a Convicted Felon) (the "TARGET OFFENSES").

5. This affidavit is also made in support of a criminal complaint and arrest warrant for Travis Joseph Crawford ("CRAWFORD"), born in 1987, for violations of Title 18, United States Code, Section 2251(a) (production of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography).

6. The statements in this affidavit are based in part on information provided by law enforcement officers of the Harford County Sheriff's Office, as well as documents and reports prepared by law enforcement officers of the Harford County Sheriff's Office and the Maryland State Police ("MSP"), Special Agents of the Bureau of Alcohol Tobacco Firearms and Explosives ("ATF"), and on my experience and background as a Special Agent of HSI. Since this affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES are located in the TARGET LOCATIONS.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

7. Based upon my experience in child exploitation investigations and upon information

provided to me by other law enforcement officers, the following can be true of child molesters/child pornographers:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms, have forums dedicated to the trafficking of child pornography images. Individuals who utilize these

types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

8. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

d. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet and its World Wide Web afford collectors of child pornography

several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo!, Google, Inc., Facebook, Dropbox, and Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including e-mail, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

f. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

g. Based on traits shared by collectors, the use of e-mail, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the production and possession of child pornography will be found in the TARGET LOCATIONS notwithstanding the passage of time.

h. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

i. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

j. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

k. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of

video files and/or hundreds of thousands of image files.

l. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

SUMMARY CONCERNING POSSESSORS OF FIREARMS

9. From speaking to Special Agents of the ATF, I have learned the following:

a. Possessors of illegal firearms, ammunition often acquire those firearms and ammunition either in their own names, or in names other than their own to avoid detection by government agencies and law enforcement. Even though these items are obtained in other people's names, the unlawful possessors actually own and continue to use these firearms and exercise dominion and control over them and related accessories. Possessors of illegal firearms and ammunition commonly maintain books, records, receipts, notes, ledgers, or other papers related to the transportation, ordering, acquisition, sale and distribution of illegal firearms and ammunition, and related accessories. Possessors of illegal firearms and ammunition often will store the above mentioned books, records, receipts, notes, ledgers and other papers related to the transportation, ordering, sale, distribution and acquisition of illegal firearms, ammunition, and related accessories in digital format on their computers or cellphones. They also commonly will take and keep photographs of illegal firearms and ammunition in their possession or in digital format on their computers and/or cellular phones, which they may keep on or about their person and/or vehicles or residences. Illegal possessors of firearms and ammunition often will use their computers or cellphones to acquire firearms, ammunition, and related accessories for their possession through the internet.

b. Possessors of illegal firearms, ammunition and/or unregistered NFA devices often utilize cellphone communications or computers to further their criminal activities by coordinating the distribution of assets, distributing, or concealing the illegal proceeds of their activities, and coordinating other efforts of co-conspirators. Possessors of illegal firearms and/or unregistered NFA devices commonly utilize cellphones, cellular telephone technology, or computers to communicate and remain in contact with co-conspirators. Possessors of illegal firearms and,/or unregistered NFA devices will often engage in face-to-face meetings with co-conspirators and/or sources of illegal firearms and unregistered NFA devices, and in doing so, often bring their cellphones with them.

APPLE

10. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). The services include email, instant messaging, and file storage.

11. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

12. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services and can also be used to store iOS device backups and data associated with third-party apps. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

13. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and

web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for Kik, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

GOOGLE

14. Google provides numerous free services to the users with a Google profile. Some of services include, Gmail, Google Hangouts, Google Wallet, Google+, Google Drive, Picasa Web Albums, and YouTube. Gmail is a web-based email service that can also be accessed via mobile apps. In 2017, Gmail comes with 15GB of free storage and users can receive emails up to 50 megabytes in size, including attachments, while they can send emails up to 25 megabytes. In order to send larger files, users can insert files from Google Drive into the message. Emails remain in an active Gmail account until deleted by the user. Google Hangouts is a communication platform which includes instant messaging, video chat, and SMS and Voice Over IP (VOIP) features service that provides both text and voice communication. Google Hangouts allows conversations between two or more users. Chat histories are saved online, allowing them to be synced between devices. Google Wallet is a mobile payment system that allows its users to store debit cards, credit cards, loyalty cards and gift cards, among other things, on their mobile phones. Google+ is a social networking service. Google Drive is a file storage and synchronization service, which provides users with cloud storage, file sharing, and collaborative editing. Picasa Web Albums is an image hosting and sharing web service that allows users with a Google account to store and share images

for free. YouTube is a free video sharing website that allows users upload, view and share videos.

PROBABLE CAUSE

15. On November 30, 2020, Harford County Sheriff's Office Deputies Hayes, Claridge and Price responded to a call for a wanted subject at [redacted] Edgewood, Maryland. When the deputies arrived at the apartment, they could hear a male voice saying, "Where is my gun?" As the deputies answered the door, resident [redacted] handed them a firearm wrapped in a towel. The deputies identified and arrested the subject, Travis Crawford ("CRAWFORD"), who was determined to be the only male in the apartment. Crawford was wanted for firearm related offenses based on a warrant that was obtained by the MSP on September 30, 2020. The firearm seized on November 30, 2020 was identified as a Taurus PT140 Pro, with serial number SEW22675, and was fully loaded with one round in the chamber.

16. While at the residence, Deputy Hayes interviewed [redacted] [redacted] told Deputy Hayes that she was CRAWFORD's girlfriend, and that she found a video on CRAWFORD's phone depicting CRAWFORD touching [redacted] 13-year old [redacted] ("Jane Doe"),[1] while Jane Doe was asleep. [redacted] told Deputy Hayes that she used her phone to record this video and other videos that were playing on CRAWFORD's phone. Deputy Claridge seized CRAWFORD's phone, a black **Apple iPhone 7, IMEI: 354916095756655**, in a black case with a clear back (the TARGET DEVICE), which was on CRAWFORD's person at the time of his arrest.

17. On December 1, 2020, Harford County Sheriff's Office Detective David Skica interviewed [redacted] [redacted] showed Detective Skica multiple videos on her phone depicting what appeared to be CRAWFORD touching Jane Doe on and about her buttocks while she appeared to be sleeping, as well as videos of Jane Doe nude in the bathroom. [redacted] stated that the videos

[1] [redacted]

appeared to have been taken [redacted], both in Jane Doe's bedroom and in the [redacted] bathroom.

18. On December 1, 2020, Harford County Sheriff's Office Detective Christine Scurto met with CRAWFORD at the Harford County Detention Center prior to his release. CRAWFORD provided the contact phone number 443-567-1403.

19. On December 2, 2020, Jane Doe was interviewed at the Harford County Child Advocacy Center. Jane Doe did not disclose any knowledge of being abused or recorded by anyone in her family or social circle.

20. On December 2, 2020, Detective Skica interviewed [redacted] again. [redacted] stated that [redacted] stated that she used CRAWFORD's finger to unlock his phone while he was intoxicated and asleep. [redacted] stated that she was looking for evidence of CRAWFORD being unfaithful in their relationship.

21. On December 4, 2020, Detective Skica sought a state search warrant for the examination of the TARGET DEVICE. The warrant was approved and signed by the Honorable Mimi R. Cooper, Judge of the District Court for Harford County, Maryland.

22. After [redacted] provided consent to search the contents of her phone, a forensic extraction of her iPhone was initiated by MSP Detective Adam LeCompte on December 4, 2020. I received and reviewed a copy of the Cellebrite Reader report generated by Detective LeCompte. I noted the contact "Travis (angry face emoji)" with the phone number 443-567-1403 in the phone's contact list.[2] I found a Messages chat log between the user of the iPhone and the contact "Travis

[2] On February 16, 20201, I spoke to [redacted] who confirmed that the phone number 443-567-1403 belonged to Travis Crawford in November 2020, and was the number she used to contact him.

(angry face emoji)" starting on August 5, 2020 and ending on November 30, 2020. [redacted]

[redacted]

23. I reviewed the videos included in the extraction. All of the following videos described below were videos that [redacted] showed Detective Skica on December 1, 2020 and identified CRAWFORD and Jane Doe as being depicted, and the videos all appear to show footage recorded by one device recording what was playing on a second device:

a. The video titled, "IMG_2640.MOV", shows the date "July 16 6:51 AM", and the location "Edgewood" at the top of screen. This video depicts Jane Doe, sleeping on her stomach, wearing blue shorts. A man's left hand, with a ring on the pinky finger, enters the frame and touches Jane Doe on and around the genital area and buttocks.

b. The video titled, "IMG_2638.MOV", shows the date "July 19 6:43AM", and the location "Edgewood" at the top of screen. This video depicts Jane Doe, wearing blue shorts and laying on her stomach, sleeping A man's left hand enters the frame and touches Jane Doe on and around the genital area and buttocks. The man has a tattoo on the inside of his left wrist.

c. The video titled, "IMG_2642.MOV", shows the date "Today 12:46 AM", and the location "Edgewood" at the top of screen. This video depicts CRAWFORD placing the camera low to the ground and angled upward. CRAWFORD then stands up and appears to manipulate the watch on his right wrist, and then reaches down to adjust the angle of the camera. CRAWFORD's face can be seen clearly during the video.

d. The video titled, "IMG_2630.MOV", shows the date "Today 12:49 AM", and the location "Edgewood" at the top of the screen. This video depicts Jane Doe, in a bathroom getting undressed and into the shower. Jane Doe then opens the shower curtain and steps out of the shower, completely nude. The camera placement appears to near the ground and angled up toward Jane Doe.

24. On January 22, 2021, an administrative summons was sent to Apple for information for accounts associated with the phone number **443-567-1403.** On January 28, 2020, Apple responded with the following information:

Apple ID:	**coldhearted1219@gmail.com**
DS ID:	11764867435
First Name:	Thomas
Last Name:	Jones
Address:	275 center deen ave, Edgewood, Maryland

	21001
Two-Factor Authentication Phone:	14435671403
iCloud Backup (iOS Devices):	No
iCloud Photos:	Yes
iCloud Drive:	Yes
Apple ID:	**twothree04@icloud.com**
DS ID:	17283723117
First Name:	Antonio
Last Name:	Jones
Address:	275 center seen, Aberdeen, Maryland 21001
Two-Factor Authentication Phone:	14435671403
iCloud Backup (iOS Devices):	Yes
iCloud Photos:	Yes
iCloud Drive:	Yes

25. The Apple response included device information for a black iPhone 7 associated with **twothree04@icloud.com**. The Apple response also included Apple Media Services data for the individual "Travis Crawford" associated with **coldhearted1219@gmail.com**, with an address of "275 center deen ave, Edgewood, MD 21001," and an IP login of 73.129.198.218 on May 19, 2020.

26. A search of publicly available databases showed that CRAWFORD resided at 275 Center Deen Ave, Aberdeen, Maryland in 2019.

27. On February 8, 2020, an administrative summons was sent to Google for information pertaining to the e-mail account **coldhearted1219@gmail.com.** On February 8, 2020, Google responded with the following information:

Google Account ID:	35356461641
Name:	Thomas Jones
E-Mail:	coldhearted1219@gmail.com
Account Created:	2015-11-03 00:54:38 UTC
Recovery SMS:	14107028542
IP Activity:	2020-05-29 00:06:52 UTC, IP Login 73.129.198.218 (the same IP address that accessed the coldhearted1219@gmail.com iCloud account on May 19, 2020)

28. On February 10, 2020, I physically examined the TARGET DEVICE and observed

the IMEI 354916095756655 printed on the SIM card tray.

TRAVIS CRAWFORD'S PRIOR CONVICTIONS

29. Prior to November 30, 2020, CRAWFORD had been convicted of a crime carrying a penalty of greater than one year, and his civil rights had not been restored following that conviction.

30. On August 18, 2010, CRAWFORD was convicted of CDS Possession Not Marijuana in the Circuit Court for Harford County, under case number 12-K-10-000550. CRAWFORD was sentenced to a jail term of 3 years and 6 months, with all but 1 year and 6 months suspended.

31. Based on a review of the Maryland Judicial Case Search website, CRAWFORD was convicted of Assault-2nd Degree and Malicious Destruction of Property/Value Less Than $1,000 on April 24, 2017, in the District Court for Harford County, under case number 12-K-16-000385.

SUMMARY

32. Based on the facts detailed above, as well as my training and experience, Crawford appears to have a sexual interest in children that includes surreptitious recordings of a minor female, engaging in sexual touching of a sleeping minor female, producing videos of such conduct, and saving the videos. Further, Crawford maintains and controls at least two email accounts.

33. Based on the activity detailed above, as well as my training and experience, I believe that user of the TARGET LOCATIONS is CRAWFORD. I also believe that the user/owner of the TARGET LOCATIONS (CRAWFORD), displays characteristics common to individuals who have a sexual interest in children, and who access with the intent to view and/or, possess and produce child pornography as discussed above.

34. Based on these characteristics, and because the TARGET LOCATIONS that are the subject of this affidavit appear to be accessed, controlled, and/or created by the same person

(CRAWFORD), I respectfully submit there is probable cause that the TARGET LOCATIONS (1) contain evidence of production and/or possession of child pornography, and (2) are relevant to determine the ownership and control of the TARGET LOCATIONS. Based on my training and experience, such information may constitute evidence of the TARGET OFFENSES because the information can be used to identify the account's user or users.

CONCLUSION

35. Based upon the foregoing information set forth in this application, I respectfully submit there is probable cause to believe that CRAWFORD violated Title 18, United States Code, Section 2251(a) (production of child pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography).

36. Even though a member of the Harford County Sheriff's Office obtained a search warrant for the TARGET PHONE, based on the advice of Assistant United States Attorney Paul Budlow, and out of an abundance of caution, it was decided to apply for the issuance of a federal search warrant requested herein.

37. Based on the foregoing information, I have probable cause to believe that contraband, and evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES as set forth herein and in Attachments B1, B2, and B3, are currently contained in the TARGET LOCATIONS, more fully described in Attachments A1, A2, and A3. I therefore respectfully request that the search warrant be issued authorizing the search of the TARGET PHONE and TARGET LOCATIONS for the items described above and in Attachments B1, B2, and B3, and authorizing the seizure and examination of any such items found therein.

38. WHEREFORE, I respectfully request that the Court issue a search warrant to search the locations listed in Attachment A1, A2, and A3 of this affidavit, and to seize any information

located pursuant to the search as described in Attachment B1, B2, and B3.

Peter T. Baish
Peter T. Baish, Special Agent
Homeland Security Investigations

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and Fed. R. Crim. P. 41(d)(3) this 18 day of February, 2021.

Honorable Thomas M. DiGirolamo
United States Magistrate Judge
District of Maryland